(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 December 2002 (05.12.2002)

PCT

(10) International Publication Number
WO 02/098054 A1

(51) International Patent Classification[7]: H04L 9/32

(21) International Application Number: PCT/US02/16801

(22) International Filing Date: 28 May 2002 (28.05.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/294,499	29 May 2001 (29.05.2001)	US
60/294,493	29 May 2001 (29.05.2001)	US
60/294,491	29 May 2001 (29.05.2001)	US
10/109,469	27 March 2002 (27.03.2002)	US

(71) Applicant *(for all designated States except US)*: **SONY ELECTRONICS INC.** [US/US]; 1 Sony Drive, Park Ridge, NJ 07656 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MARITZEN, Michael** [US/US]; 3300 Zanker Road, San Jose, CA 95134 (US). **LUDTKE, Harold, Aaron** [US/US]; 3587 Townsquare Drive, San Jose, CA 95127 (US). **YASUDA, Hiroyuki** [JP/US]; 680 Kinderkamack Road, Oradell, NJ 07649 (US). **NIWA, Kiyohiko** [JP/US]; 680 Kinderkamack Road, Oradell, NJ 07649 (US). **CHATANI, Masayuki** [JP/US]; 919 East Hilldale Boulevard, Foster City, CA 94404 (US). **TSUKAMURA, Yoshihiro** [JP/US]; 680 Kinderkamack Road, Oradell, NJ 07649 (US).

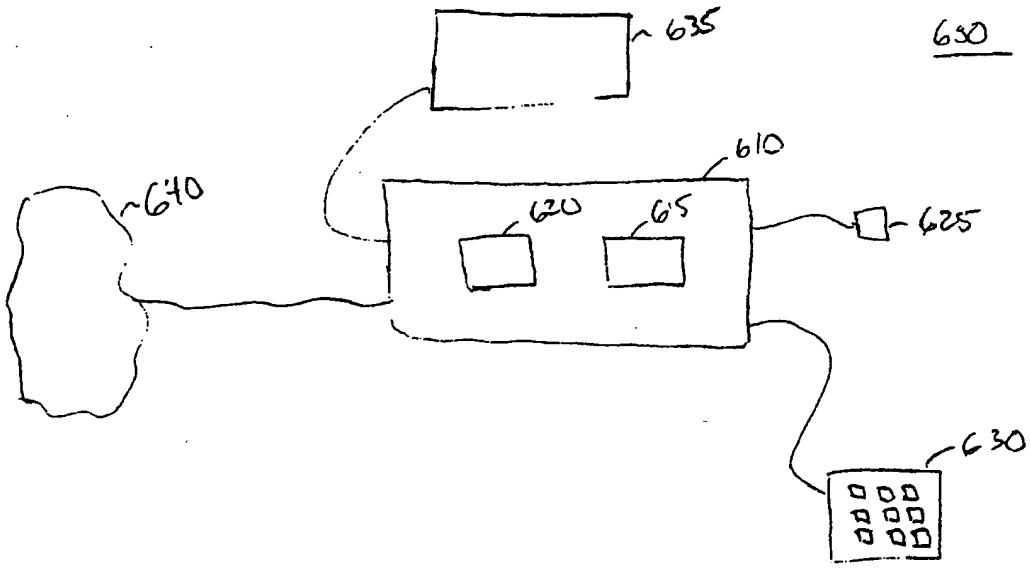
(74) Agent: **BUTT, Richard, H.**; Valley Oak Law, 5655 Silver Creek Valley Road, #106, San Jose, CA 95138 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR SECURE ENTRY AND AUTHENTICATION OF CONSUMER-CENTRIC INFORMATION



(57) Abstract: A system and method for providing a secure transaction and authentication system through a gaming console are described. The invention allows a consumer to utilize a game console (610) to conduct secure transactions and authenticate the identity of the consumer using the game console (610). In one embodiment, the invention includes a game console (610) for use by a consumer; a biometric pad (625) coupled to the game console for receiving a biometric input from the consumer to authenticate an identity of the consumer; and a control pad (630) coupled to the game console for entering information by the consumer.

WO 02/098054 A1

Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

System and Method for Secure Entry and Authentication of Consumer-Centric Information

CROSS REFERENCE TO RELATED APPLICATIONS

The present application claims benefit of U.S. Provisional Patent Application Nos. 60/294,499; 60/294,493; and 60/294,491 all filed on May 29, 2001, respectively entitled "A Method and Apparatus for Gaming Console USB Port Authentication and Authorization", "A Method and Apparatus for an Integrated Biometric Gaming Console Model", and "A PKI-Enabled Method and Apparatus for a Gaming Console User Identity and Payment Model" all listing the same inventors, both disclosures of which are hereby incorporated by reference.

BACKGROUND OF THE INVENTION

[0001] Electronic commerce is achieving widespread use. Transactions are performed everyday over the Internet and through point of sale (POS) or bank systems. Such transactions are typically performed after the person requesting access to some information is authenticated and access is given to that person's private information, such as financial, medical, or other type of restricted records. Present systems are designed to maintain the integrity of the user's credit card, debit card, and account number. However, no measures are taken to ensure the secure authentication of the user in order to prevent unauthorized access by a potential thief.

[0002] Presently, applications providing access to sensitive information are based upon information that a potential thief may appropriate with relative ease. For example, some of the information presently required to grant access to sensitive material, such as a person's Social Security Number, date of birth, or

mother maiden's name, is readily available. Once a potential thief collects any two pieces of this information, the thief may obtain access to the person's financial, medical, or other private information. In addition, most secure access systems are set up to divulge a person's entire file, once they receive the appropriate password and/or correct answers to the security questions. Therefore, a potential thief may steal the person's identity and ruin that person's credit.

[0003] Presently, existing gaming consoles or set top boxes are typically designed to be utilized with pre-purchased gaming media that physically plugs into the gaming consoles. Most existing gaming consoles are not constructed to perform financial transactions with remote devices such as point of sale, point of use, and the like.

SUMMARY OF THE INVENTION

A system and method for providing a secure transaction and authentication system through a gaming console are described. The invention allows a consumer to utilize a game console to conduct secure transactions and authenticate the identity of the consumer using the game console. In one embodiment, the invention includes a game console for use by a consumer; a biometric pad coupled to the game console for receiving a biometric input from the consumer to authenticate an identity of the consumer; and a control pad coupled to the game console for entering information by the consumer.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] The present invention is illustrated by way of example and not limitation in the figures of the accompanying drawings, in which like references indicate similar elements and in which:

[0005] **Figure 1** is a simplified block diagram of one embodiment of a secure transaction system.

[0006] **Figure 2** is a simplified block diagram of one embodiment of a privacy card for a personal transaction device.

[0007] **Figure 3** is a simplified block diagram of one embodiment of a digital wallet for a personal transaction device.

[0008] **Figure 4** is a simplified block diagram of one embodiment of a secure transaction system showing a point-of-sale terminal.

[0009] **Figure 5** is a simplified block diagram of one embodiment of a transaction privacy clearing house.

[0010] **Figure 6** illustrates one embodiment of a gaming console.

[0011] **Figure 7** illustrates another embodiment of a gaming console.

[0012] **Figure 8** illustrates one embodiment of profile information.

[0013] **Figure 9** illustrates a flow diagram for performing one embodiment of an initialization.

[0014] **Figure 10** illustrates a flow diagram for performing one embodiment of a real-time payment model.

DETAILED DESCRIPTION

[0015] In the following descriptions for the purposes of explanation, numerous details are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to one skilled in the art that these specific details are not required in order to practice the present invention. In other instances, well-known electrical structures or circuits are shown in block diagram form in order not to obscure the present invention unnecessarily.

[0016] A system and method for secure entry and authentication of consumer information via a game console allows the consumer greater flexibility in accomplishing tasks while using the game console. For example, the system and method enables secure financial transactions to be accomplished through the game console. In one embodiment, content may be acquired for the game console and utilized by the game console while payment is automatically made to a merchant during mid-stream of the transaction. In other words, the system and method enable these payments to be made in real-time and enable payment from the consumer to the merchant while the consumer is receiving the goods or consuming the services. In one embodiment, the system and method also allow for user authentication such as through biometric identification, token exchange, PIN entry, and the like. In one embodiment, the invention operates in conjunction with a secured transaction exchange, controlled content access, and the like.

[0017] Security of the user's identity may be achieved in a variety of ways. In one embodiment, a single trusted location. For example, a transaction privacy clearing house (TPCH) contains user data. The user interfaces with the TPCH using the user's transaction device. The user therefore does not fill out online

the electronic purchase forms at every product vendor's website. The TPCH acts as a financial transaction middleman, stripping off user identity information from transactions. As a result, the user's private information is not stored in several databases across the Internet and in private business networks. The secure locations where the financial data is stored minimizes the possibilities that hackers can access the data or accidental releases of the data can occur. In one embodiment, multiple secure locations are utilized for storage to prevent theft of confidential information.

[0018] **Figure 1** is a simplified block diagram of one embodiment of a secure transaction system, which may be used in electronic commerce. As illustrated in **Figure 1**, in this embodiment, a transaction privacy clearing house (TPCH) 115 interfaces a user (consumer) 140 and a vendor 125..

[0019] In this particular embodiment, a personal transaction device (PTD) 170, e.g., a privacy card 105, or a privacy card 105 coupled to a digital wallet 150, is used to maintain the privacy of the user while enabling the user to perform transactions. The personal transaction device 170 may include a window interface, a privacy card, a digital wallet, a point of sale terminal, a laptop computer, a desktop computer, a PDA, or any other device under the control of the user 140.

[0020] The personal transaction device 170 provides an interface for the user to exchange information. This exchange of information may include but is not limited to the user 140 receiving audio and/or visual content, instructions, requests, and the like from the personal transaction device 170. Further, this exchange of information may also include but is not limited to the personal

transaction device 170 receiving instructions, payment authorization, authentication, and the like from the authorized user 140.

[0021] In one embodiment, the personal transaction device 170 is a fixed window interface within kiosk at a mall. Both the mobile window interface and the fixed window interface may be available for use by the general public if installed on public transportation or in public areas. In one embodiment, both the mobile window interface and the fixed window interface display information to the user and allows information to be entered by the user through the same display. In one embodiment, a user authentication mechanism such as a fingerprint recognition unit or other mechanism may be built directly into the card. In addition, the personal transaction device 170 may also contain wireless data communication, data storage and communication protocols for selectively communicating with outside devices such as a digital wallet described herein, point-of-sale terminal, or personal computer, and digital televisions.

[0022] In one embodiment, the personal transaction device 170 is configured to manage and control access to content and/or transactions received by individual accounts associated with the users of the personal transaction device. In one embodiment, the personal transaction 170 is configured to control the individual accounts by way of entering a unique biometric identifier associated with that particular account. Further, the user may select different information by entering unique biometric identifiers through the personal transaction device 170.

[0023] In an alternate embodiment, account management and control of access to content is achieved through the PTD 170. The PTD 170 may assign particular accounts with varying levels of content access and may place accounts into convenient groupings for account management.

[0024] In one embodiment, the personal transaction device 170 is configured to automatically handle contextual information and share this information with appropriate parties on behalf of the user.

[0025] In an alternate embodiment, the PTD 170 may be any suitable device that allows unrestricted access to TPCH 115. In one embodiment, the personal transaction device 170 may include a full screen that covers one side of the card. Alternately, in one embodiment in which the personal transaction device 170 is one embodiment of a privacy card, the privacy card may be coupled to device such as a digital wallet described herein, that provides a display. In one embodiment, the screen may be touch sensitive and be used for data input as well as output. In one embodiment, a user authentication mechanism such as a fingerprint recognition or other mechanism may be built directly into the card. Furthermore, the privacy card may have a wireless communication mechanism for input and output.

[0026] A variety of user interfaces may be used. In one embodiment, and input device may be incorporated on the transaction device. Alternately, a supplemental input device may be coupled to the transaction device. In one embodiment, an input device may be provided on a digital wallet coupled to a privacy card. User inputs may be provided on the point-of-sale terminals including a personal point-of-sale terminal.

[0027] The personal transaction device information is provided to the TPCH 115 that then indicates to the vendor 125 and the user 140 approval of the transaction to be performed. The transaction device utilizes an identification to maintain confidentiality of the user's identity by applying the transaction device identification and the identity of the entity performing the transaction. Thus, all

transactions, from the vendor's perspective, are performed with the transaction device.

[0028] In order to maintain confidentiality of the identity of the user 140, the transaction device information does not provide user identification information. Thus, the vendor 125 or other entities do not have user information but rather transaction device information. The TPCH 115 maintains a secure database of transaction device information and user information. In one embodiment, the TPCH 115 interfaces to at least one financial processing system 120 to perform associated financial transactions, such as confirming sufficient funds at the vendor account 125 to perform the reverse payment transaction, and transfers to the user 140 the funds required to complete the transaction. In another embodiment, the TPCH 115 interfaces to at least one financial processing system 120 to perform associated financial transactions, such as confirming sufficient funds to perform the transaction, and transfers to the vendor 125 the fees required to complete the transaction. In addition, the TPCH 115 may also provide information through a distribution system 130 that, in one embodiment, can provide a returned product to the vendor 125 from the user 140, again without the vendor 125 knowing the identification of the user 140. In addition, the TPCH 115 may also provide information through a distribution system 130 that, in one embodiment, can provide a purchased product to the user 140, again without the vendor 125 knowing the identification of the user 140. In an alternate embodiment, the financial processing system 120 need not be a separate entity but may be incorporated with other functionality. For example, in one embodiment, the financial processing system 120 may be combined with the TPCH 115 functionality.

[0029] In one embodiment, the financial processing system (FP) 120 performs tasks of transferring funds between the user's account and the vendor's account for each transaction. In one embodiment, the presence of the TPCH 115 means that no details of the transactions, other than the amount of the transactions and other basic information, are known to the FP 120. The TPCH 115 issues transaction authorizations to the FP 120 function on an anonymous basis on behalf of the user over a highly secure channel. The FP 120 does not need to have many electronic channels receiving requests for fund transfer, as in a traditional financial processing system. In one embodiment, a highly secure channel is set up between the TPCH 115 and the FP 120; thus, the FP 120 is less vulnerable to spoofing.

[0030] In one embodiment, the TPCH 115 contacts the FP 120 and requests a generic credit approval of a particular account. Thus, the FP 120 receives a minimal amount of information. In one embodiment, the transaction information, including the identification of goods being purchased with the credit need not be passed to the FP 120. The TPCH 115 can request the credit using a dummy charge ID that can be listed in the monthly financial statement sent to the user, so that the user can reconcile his financial statement. Further, the personal transaction device 170 can include functionality to cause the financial statement to convert the dummy charge ID back to the transactional information so that the financial statement appears to be a conventional statement that lists the goods that were purchased and the associated amount charged.

[0031] A display input device 160 (shown in phantom) may be included to enable the user, or in some embodiments the vendor 125, to display status and

provide input regarding the PTD 170 and the status of the transaction to be performed.

[0032] In yet another embodiment, an entry point 110 interfaces with the personal transaction device 170 and also communicates with the TPCH 115. The entry point 110 may be an existing (referred to herein as a legacy POS terminal) or a newly configured point of sale (POS) terminal located in a retail environment. The user 140 uses the PTD 170 to interface to the POS terminal in a manner similar to how credit cards and debit cards interface with POS terminals. The entry point 110 may also be a public kiosk, a personal computer, or the like.

[0033] In another embodiment, the PTD 170 interfaces through a variety of interfaces including wireless interfaces such as BlueTooth and infrared transmission; contactless transmission such as FeliCa and AmexBlue; and plug-in port transmission such as USB and RS-232C. A stand-in processor 155 (STIP) can interface with the PTD 170 in the event that the connection between the front end and the back end is disrupted for any reason. This way, the PTD 170 can gain authorization for a specified floor limit without necessarily receiving authorization from the back end. Further, this limits the amount of authorization thus minimizing fraud and insufficient funds.

[0034] The system described herein also provides a distribution functionality 130 whereby products purchased via the system are distributed. In one embodiment, the distribution function 130 is integrated with the TPCH 115 functionality. In an alternate embodiment, the distribution function 130 may be handled by a third party. Utilizing either approach, the system ensures user privacy and data security. The distribution function 130 interacts with the user

through PTD 170 to ship the product to the appropriate location. A variety of distribution systems are contemplated, for example, electronic distribution through a POS terminal coupled to the network, electronic distribution direct to one or more privacy cards and/or digital wallets, or physical product distribution. In one embodiment for physical product distribution, an "anonymous drop-off point", such as a convenience store or other ubiquitous location is used. In another embodiment, it involves the use of a "package distribution kiosk" that allows the user to retrieve the package from the kiosk in a secure fashion. However, in one embodiment, the user may use PTD 170 to change the shipping address of the product at any time during the distribution cycle.

[0035] A user connects to and performs transactions with a secure transaction system (such as shown in **Figure 1**) through a personal transaction device (PTD) that has a unique identifier (ID). In one embodiment, a privacy card is used. In an alternate embodiment a digital wallet is used. In yet another alternate embodiment, a privacy card in conjunction with a digital wallet are used.

[0036] **Figure 2** is a simplified block diagram of one embodiment of a privacy card 205 for a personal transaction device. As illustrated in **Figure 2**, in one embodiment, the card 205 is configured to be the size of a credit card. The privacy card includes a processor 210, memory 215 and input/output logic 220. The processor 210 is configured to execute instructions to perform the functionality herein. The instructions may be stored in the memory 215. The memory is also configured to store data, such as transaction data, user preferences, and the like. In one embodiment, the memory 215 stores the transaction ID used to perform transactions in accordance with the teachings of

the present invention. Alternately, the processor may be replaced with specially configured logic to perform the functions described here.

[0037] The input/output logic 220 is configured to enable the privacy card 205 to send and receive information. In one embodiment, the input/output logic 220 is configured to communicate through a wired or contact connection. In another embodiment, the logic 220 is configured to communicate through a wireless or contactless connection. A variety of communication technologies may be used.

[0038] In one embodiment, a display 225 is used to generate bar codes scanable by coupled devices and used to perform processes as described herein. The privacy card 205 may also include a magnetic stripe generator 240 to simulate a magnetic stripe readable by devices such as legacy POS terminals.

[0039] In one embodiment, biometric information, such as fingerprint recognition, is used as a security mechanism that limits access to the card 205 to authorized users. A fingerprint touch pad and associated logic 230 is therefore included in one embodiment to perform these functions. Alternately, security may be achieved using a smart card chip interface 250, which uses known smart card technology to perform the function.

[0040] Memory 215 can have transaction history storage area. The transaction history storage area stores transaction records (electronic receipts) that are received from POS terminals. The ways for the data to be input to the card include wireless communications and the smart card chip interface which functions similar to existing smart card interfaces. Both of these approaches presume that the POS terminal is equipped with the corresponding interface and can therefore transmit the data to the card.

[0041] Memory 215 can also have user identity/account information block. The user identity/account information block stores data about the user and accounts that are accessed by the card. The type of data stored includes the meta account information used to identify the account to be used.

[0042] In another embodiment, the memory 215 also stores the embedded content received by the privacy card.

[0043] In another embodiment, the memory 215 also stores the account management information such as categories and the account access levels of content.

[0044] In another embodiment, the memory 215 also stores the contextual information gathered by the personal transaction device.

[0045] In yet another embodiment, the memory 215 also stores profile information that is initialized by the user and reflects the user's preferences for mid-stream payments to the merchant.

[0046] **Figure 3** is a simplified block diagram of one embodiment for a personal transaction device 305. As illustrated in **Figure 3**, the PTD 305 includes a coupling input 310 for the privacy card 205, processor 315, memory 320, input/output logic 325, display 330, and peripheral port 335. The processor 315 is configured to execute instructions, such as those stored in memory 320, to perform the functionality described herein. Memory 320 may also store data including financial information, eCoupons, shopping lists, embedded content, and the like. The PTD 305 may be configured to have additional storage. In one embodiment, the additional storage is in a form of a card that couples to the device through peripheral port 310.

[0047] In one embodiment, the privacy card 205 couples to the PTD 305 through port 310; however, the privacy card 205 may also couple to the PTD 305 through another form of connection including a wireless connection.

[0048] Input/output logic 325 provides the mechanism for the PTD 305 to communicate information. In one embodiment, the input/output logic 325 provides data to a point-of-sale terminal or to the privacy card 205 in a pre-specified format. The data may be output through a wired or wireless connection.

[0049] The PTD 305 may also include a display 330 for display of status information to the user.

[0050] The transaction device enhances security by authenticating the user of the card prior to usage such that if that transaction device is useless in the hands of an unauthorized person. One means of authentication is some type of PIN code entry. Alternatively, authentication may be achieved by using more sophisticated technologies such as a biometric solution. This biometric solution can include fingerprint recognition, voice recognition, iris recognition, and the like. In addition, in one embodiment in which multiple transaction devices are used, it may be desirable to configure the first device to enable and program the second device in a secure manner. Thus, the means of communication between the first device in the second device may include mutual device verification such that an unauthorized first device may not be used to enable a particular second device that does not belong to the same or authorized user.

[0051] In one embodiment, the transaction device, point of sale terminals and/or TPCH may function to verify the authenticity of each other. For example the transaction device may be configured to verify the legitimacy of the point-of-

sale terminal and/or TPCH. A variety of verification techniques may be used. For example, in one embodiment, the public key infrastructure may be used to verify the legitimacy of the user.

[0052] Communication protocols include those that allow the digital wallet to specify which of several possible data structures to use for a transaction and communication protocols that allow the digital wallet and other devices to securely share data with the transaction device. The transaction device may represent a single account such as a particular credit card, or it may represent multiple accounts such as a credit card, telephone card, and debit card.

[0053] In one embodiment, the transaction device is intended to be the means by which the user interfaces with the invention. In one embodiment, the transaction device stores e-commerce related data on behalf of the user including transaction histories, meta account information needed to carry out a transaction using the transaction privacy clearinghouse function of the system, and various content. In one embodiment, the meta account information may be an abstaction of the user's real identity as opposed to the actual user's name, address, etc. For example, the TPCH keeps records of the user's real bank account numbers, but assigned a different number for use by retailers and point-of-sale terminals. For example, and actual Bank Account No. may be 1234 0000 9876 1423 could be represented as 9999 9999 9999 9999. This number, in association with the transaction card's identification, could enable the TPCH to know that the bank account No. 1234 0000 9876 1423 was actually the account being used.

[0054] The purpose of this data is to abstract the user's identity while at the same time providing the necessary information for the transaction to be completed.

[0055] In one embodiment, the personalization process of the transaction device may be as described below. In this example, the transaction device is a digital wallet. The user turns on the transaction device. This can be accomplished by touching the finger print recognition pad or simply turning a switch. The transaction device performs at start a procedure, and recognizes that it has not yet been personalized. Thus, it first prompt the user to enter the secret pin code. If the pin code entry fails, the user is prompted again. Ideally the user is given a finite number of chances to enter the data. After the last failure, the device may permanently disable itself and thus becomes useless. It may also display a message requesting that the transaction device be returned to an authorized facility.

[0056] Assuming a successful pin code entry, the user may then be prompted to answer several of the security questions which were entered into the transaction device at processing center. Some of these questions might require data entry, and others might be constructed as simple multiple-choice, with both the correct as well as incorrect answers supplied. Assuming successful response to these questions, the user may then be prompted to enter secure personal identification information such as fingerprint data. In one embodiment, in which the fingerprint data is used, the user is prompted to enter fingerprint data by successively pressing one or more fingers against the recognition pad. The device prompt the user for each fingerprint that must be entered, for example, using a graphical image of a hand with the indicated finger.

[0057] The fingerprint data entry process may be performed at least twice to confirm that the user has entered the correct data. If confirmation succeeds, the device writes the fingerprint image data into their write once memory, or other memory that is protected from accidental modification. If confirmation fails, the user is prompted to start over with entry. Failure to reliably enter the fingerprint data after a finite number of tries will result in the device permanently disabling itself, and optionally providing an on-screen message to the user to go to secure processing facility such as a bank to complete the process. After successful personalization, the device is then ready to be used for the initial set of services that the user requested during the registration process. Once the device has been initialized for secure transactions, additional services could be downloaded to the device.

[0058] In one embodiment, the authentication of the identity of the user and selecting particular information by the user may be combined by the user providing a unique biometric input which corresponds to the particular selected information.

[0059] One embodiment of the system that utilizes a point-of-sale terminal is shown in **Figure 4**. In this embodiment, the privacy card 405 interfaces with the point-of-sale terminal 410 and that point of sale terminal 410 communicates with that TPCH 415. That TPCH 415 interfaces with the financial processing system 420, the vendor 425 and the distribution system 430. The point-of-sale terminal may be an existing or newly configured point-of-sale terminal located in a retail environment. The user 440 uses the privacy card 405 to interface to the point-of-sale terminal a manner similar to how credit cards and debit cards interface with point-of-sale terminals. Alternately, a digital wallet 450 may be used by

itself or with the privacy card 405 to interface to the point-of-sale terminal 410. Alternately, a memory device may be utilized solely as the interface with that point-of-sale terminal 410.

[0060] One embodiment of the TPCH is illustrated in **Figure 5**. In one embodiment, the TPCH 500 is located at a secure location and is accessible to the transaction device. The TPCH 500 functions to provide the user with authorization to perform transactions without compromising the user's identity. The TPCH 500 may be embodied as a secure server connected to the transaction device in some form of direct connection or alternately a format in direct connection over the Internet or point-of-sale network.

[0061] Incoming communications mechanism 505 and outgoing communications mechanism 510 are the means of communicating with external retailers and vendors, as well as the transaction device such as the digital wallet. A variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless, cellular signals, etc.

[0062] The TPCH agent 515 handles system management and policy control, informs their core functionality of the TPCH 500. In one embodiment, within the entire system, there is one clearinghouse agent, which resides permanently at the clearinghouse. Among the responsibilities handled by the agent include internal system management functions such as data mining, financial settlement and allocation of payments to internal and external accounts, embedded content management, and registration of new users joining the system.

[0063] The security management functions 520 ensure secure communications among the component internal to the TPCH 500 and the entities external to the TPCH 500. This function includes participating in secure

communications protocols to open and maintain secure connections. This ensures that only authorized entities are allowed to access to data and that only authorized transaction devices can execute transactions against a user's account.

[0064] The TPCH agent 515 also provides a direct marketing and customer contact service 525, which in one embodiment is a data access control mechanism and maintain separate, secure access between various client and their databases. The data access control mechanism ensures that vendors have access only to the appropriate data in order to carry out the tasks of the system. One of the key features at the TPCH 500, the ability to carry out focused direct marketing while maintaining the privacy and identity protection of consumer, is handled by this mechanism.

[0065] The TPCH agent 515 can be configured to actively look for content on behalf of the user as well as filter out unwanted incoming information. In one embodiment, the data may be described by XML and the agent may operate via Java applets.

[0066] In one embodiment, **Figure 6** illustrates a gaming console system 600. The gaming console system 600 includes a game console 610, a biometric pad 625, a control pad 630, a display 635, and a network 640. The game console 610 includes a processor 620 and a memory module 615. The game console 610 is connected to the biometric pad 625, the control pad 630, the display 635, and the network 640. The gaming console system 600 is configured to be operated as a personal transaction device for use by the consumer.

[0067] In one embodiment, the control pad 630 is utilized to control action of the animated games as well as enter, edit, and select information for use with the gaming console system 600.

[0068] In one embodiment, the biometric pad 625 is configured to receive a fingerprint of the consumer and deliver the fingerprint information to the game console 610. The use of the biometric pad 625 allows for authentication of the consumer's identity through a convenient and unobtrusive source. In another embodiment, the consumer may also be requested to enter a PIN through the control pad 630 to further authenticate the identity of the consumer.

[0069] In one embodiment, the display 635 is configured to display the animated games and information for the consumer. The information for the consumer may include profile information which has been entered, edited, and/or stored by the consumer. In one embodiment, viewing profile information or any information that is separate from the graphics associated with the gaming aspects are shown in a pop-up style window that may be moved around the display 635 to facilitate custom viewing.

[0070] In one embodiment, the network 640 may include the Internet, a local area network, a wide area network, a telephone network, and the like. In addition, the network 640 may also utilize wireless technology such as infrared, radio frequency, microwave, and cellular technologies.

[0071] In one embodiment, the memory module 615 stores profile information such as personal information of the consumer, software licenses owned by the consumer, preferences of the consumer, and the like.

[0072] The gaming console system 600 is configured to be utilized with a secure transaction system as described in **Figures 1** and **5**. By authenticating

the identity of the consumer, the consumer is able to conduct secure transactions such as purchasing products and/or services while making automatically making payments mid-stream while utilizing the gaming console system 600. Further, valid licenses may be confirmed in real-time while games are played on the gaming console system 600 to prevent unauthorized use of gaming software.

[0073] In yet another embodiment, **Figure 7** illustrates a gaming console system 700. The gaming console system 700 includes a game console 710, a token adapter 725, a control pad 730, a display 735, a network 740, and a token 745. The game console 710 includes a processor 720 and a memory module 715. The game console is connected to the token adapter 725, the control pad 730, the display 735, and the network 740. The gaming console system 700 is configured to be operated as a personal transaction device for use by the consumer.

[0074] In one embodiment, the control pad 730 is utilized to control action of the animated games as well as enter, edit, and select information for use with the gaming console system 700.

[0075] In one embodiment, the token adapter 725 is configured to receive the token 745 and to deliver authentication information to the game console 710. The use of the token adapter 725 allows for authentication of the consumer's identity by insertion of the token 745 into the token adapter 725. The token 745 is analogous to a physical key. However, unlike most traditional keys, the token 745 includes a storage module that storess information that uniquely identifies the consumer. In another embodiment, the consumer may also be requested to enter a PIN through the control pad 730 to further authenticate the identity of the

consumer. In one embodiment, the token 745 also stores profile information related to the consumer. This profile information may include personal information of the consumer, software licenses owned by the consumer, preferences of the consumer, and the like.

[0076] In one embodiment, the display 735 is configured to display the animated games and information for the consumer. The information for the consumer may include profile information which has been entered, edited, and/or stored by the consumer. In one embodiment, viewing profile information or any information that is separate from the graphics associated with the gaming aspects are shown in a pop-up style window that may be moved around the display 735 to facilitate custom viewing.

[0077] In one embodiment, the network 740 may include the Internet, a local area network, a wide area network, a telephone network, and the like. In addition, the network 740 may also utilize wireless technology such as infrared, radio frequency, microwave, and cellular technologies.

[0078] In one embodiment, the memory module 715 stores profile information such as personal information of the consumer, software licenses owned by the consumer, preferences of the consumer, and the like.

[0079] The gaming console system 700 is configured to be utilized with a secure transaction system as described in **Figures 1** and **5**. By authenticating the identity of the consumer, the consumer is able to conduct secure transactions such as purchasing products and/or services while making automatically making payments mid-stream while utilizing the gaming console system 700. Further, valid licenses may be confirmed in real-time while games

are played on the gaming console system 700 to prevent unauthorized use of gaming software.

[0080] **Figure 8** illustrates one embodiment of a stored profile information 800. The stored profile information 800 may be locally stored within a personal transaction device or remotely stored at a secured location such the token 745 (**Figure 7**). The stored profile information 800 may include information transactional information such as merchant list 810, consumer account list 820, increment of payment 830, and total transaction cost 840. In one embodiment, the merchant list 810 identifies a list of merchants that the consumer wishes to utilize for the method and system of mid-stream payment. The consumer account list 820 identifies a corresponding account associated with each merchant within the merchant list for payment to the associated merchant. The consumer account list 820 may include credit cards, checking accounts, savings accounts, brokerage accounts, monthly services, and the like.

[0081] The stored profile information 800 may also include user preferences, parental content access control, authorized use of software through licenses, and the like.

[0082] The increment of payment 830 is associated with each merchant and allows for a predetermined amount of money to be transferred to the merchant for each discrete payment using the method and system of mid-stream payment. The total transaction cost 840 is associated with each merchant and allows for a predetermined maximum amount of money to be transferred to the merchant for the entire transaction using the method and system of mid-stream payment.

[0083] For example, under the merchant list 810, the music distribution company corresponds to the Visa account information under the consumer

account 820. Similarly, the book store company under the merchant list 810 corresponds with the bank account under the consumer account 820. The $5.00 increment of payment 830 associated with the music distribution company under the merchant list 810 sets $5.00 as the amount to be transferred to the music distribution company. Additionally, the $15.00 limit under the total transaction cost 840 associated with the music distribution company under the merchant list 810 limits the total amount to be transferred from the consumer to the music distribution company. Similarly, the $50.00 limit under the total transaction cost 840 associated with the book store company limits the amount to be transferred from the consumer to the book store company. In one embodiment, the total transaction cost 840 may be set aside with authorization from the consumer.

[0084] In one embodiment, the method and system of mid-stream payment allows for payment to a merchant from a consumer in real-time based on a pay per minute scheme, pay per byte scheme, pay per subscription rate scheme, and pay per limited use scheme. The pay per minute scheme is analogous to a phone card system. The pay per byte scheme is analogous to a paying a fee based on the amount of content consumed by the consumer. The pay per limited use scheme is analogous to a single use model where the consumer connects once to play an unlimited number of games. The pay per subscription rate scheme is analogous to a flat rate buffet type of use where the consumer is able to use in an unlimited fashion.

[0085] In one embodiment, the method and system of mid-stream payment includes the ability to automatically transfer funds from the consumer to the merchant during the purchase of goods or services. Further, the method and system of mid-stream payment can be configured to not need intervention from

the consumer and can avoid interruption of the delivery of goods or services to the consumer. In some cases, additional confirmation by the consumer may be needed to protect the consumer from an unauthorized transfer of funds. This confirmation may include verifying the authenticity of the consumer's identity. Further, the method and system of mid-stream payment may compensate the merchant while keeping the consumer's identity anonymous.

[0086] The flow diagram as depicted in **Figures 9** and **10** are merely one embodiment of the invention. The blocks may be performed in a different sequence without departing from the spirit of the invention. Further, blocks may be deleted, added or combined without departing from the spirit of the invention.

[0087] **Figure 9** illustrates one embodiment of a user initialization of the mid-stream model. In Block 900, a link is established between the consumer and the consumer's profile information. In Block 910, authentication of the identity of the consumer is confirmed by either receiving a token, receiving a PIN, receiving a biometric parameter, or the like. In Block 920, profile information is entered and/or edited. An exemplary form of profile information is described and shown in **Figure 8**. In Block 930, the profile information is stored either locally within the device or remotely on the token 745 (**Figure 7**).

[0088] **Figure 10** illustrates one embodiment of consumer authentication through a game console and use of the game console for a financial transaction. In Block 1000, authentication of the identity of the consumer is confirmed by either receiving a token, receiving a PIN, receiving a biometric parameter, or the like. In Block 1010, content is transferred from the merchant to the consumer through a game console. In Block 1020, a secure link is automatically established between the merchant bank and the selected consumer account

designated by the consumer through the profile information without additional interaction by the consumer or the merchant. The merchant is matched with a merchant on the merchant list 810 (**Figure 8**) within the profile information. In one embodiment, this link is established during the transfer of the content from the merchant to the consumer. In Block 1030, a payment request is automatically sent from the merchant to the consumer. In Block 1040, an increment of payment is searched within the profile information for this particular merchant. The increment of payment is the payment amount. If the increment of payment is not available for this particular merchant, then the payment request contains a payment amount.

[0089] In Block 1050, a check is performed to determine if the summation of payment amounts for this entire transaction exceeds the total transaction cost which is preselected by the consumer in the profile information. If the summation of these payment amounts exceeds the total transaction cost, the consumer is asked to provide confirmation in Block 1060. After this confirmation or if the summation of these payment amounts do not exceed the total transaction cost, then funds for the payment amount are transferred from the consumer account to the merchant in Block 1070. In Block 1080, if there are additional payments requested by the merchant, the process loops back to the Block 1030.

[0090] In one embodiment, the transfer of the goods and/or services from the merchant to the consumer as described in the Block 1010 may occur during events described in the Blocks 1000, 1020, 1030, 1040, 1050, 1060, 1070, and/or 1080. In one embodiment, the consumer's true identity may remain anonymous to the merchant by utilizing secure transaction processes as

described in **Figures 1** and **5**. In one embodiment, the transactional processing of transferring funds is accomplished through secure backoffice activities and applications as described in **Figures 1** and **5**.

[0091] The foregoing descriptions of specific embodiments of the invention have been presented for purposes of illustration and description.

[0092] They are not intended to be exhaustive or to limit the invention to the precise embodiments disclosed, and naturally many modifications and variations are possible in light of the above teaching. The embodiments were chosen and described in order to explain the principles of the invention and its practical application, to thereby enable others skilled in the art to best utilize the invention and various embodiments with various modifications as are suited to the particular use contemplated. It is intended that the scope of the invention be defined by the Claims appended hereto and their equivalents.

CLAIMS

1. A game console system comprising:

a. a game console (610) for use by a consumer;

b. a biometric pad (625) coupled to the game console (610) for receiving a biometric input from the consumer to authenticate an identity of the consumer; and

c. a control pad (630) coupled to the game console (610) for entering information by the consumer.

2. The system according to Claim 1 wherein the information is a PIN.

3. The system according to Claim 1 wherein the biometric input is a finger print.

4. The system according to Claim 1 further comprising a network coupled to the game console wherein the game console is configured to perform transactions with a remote entity.

5. The system according to Claim 1 further comprising a display coupled to the game console for displaying the information in a separate area.

6. The system according to Claim 1 wherein the game console further comprising a memory module for storing a profile information related to the consumer.

7. A game console system comprising:

a. a game console (710) for use by a consumer;

b. a token adapter (725) coupled to the game console (710) for receiving information to authenticate an identity of the consumer;

c. a token (745) configured to be received by the token adapter (725) for identifying the consumer; and

d. a control pad (730) coupled to the game console (710) for entering information by the consumer.

8. The system according to Claim 7 wherein the information is a PIN.

9. The system according to Claim 7 wherein the token further comprises a memory module for storing profile information corresponding to the consumer. print.

10. The system according to Claim 7 further comprising a network coupled to the game console wherein the game console is configured to perform transactions with a remote entity.

11. The system according to Claim 7 further comprising a display coupled to the game console for displaying the information in a separate area.

12. A method of initializing comprising:

a. receiving (900) an input from a consumer on a game console;

b. matching (920) the input from the consumer with stored data; and

c. authenticating (910) an identity of the consumer.

13. The method according to Claim 12 wherein receiving the input further comprises receiving a token from the consumer and reading information from the token.

14. The method according to Claim 12 wherein receiving the input further comprises receiving a PIN from the consumer.

15. The method according to Claim 12 wherein receiving the input further comprises receiving a biometric parameter from the consumer.

16. The method according to Claim 15 wherein the biometric parameter is a fingerprint.

17. The method according to Claim 12 further comprising authenticating an identity of a merchant.

18. The method according to Claim 12 further comprising authenticating an identity of a financial institution.

19. A computer-readable medium having computer executable instructions for performing a method comprising:

a. receiving (900) an input from a consumer on a game console;

b. matching (920) the input from the consumer with stored data; and

c. authenticating (910) an identity of the consumer.

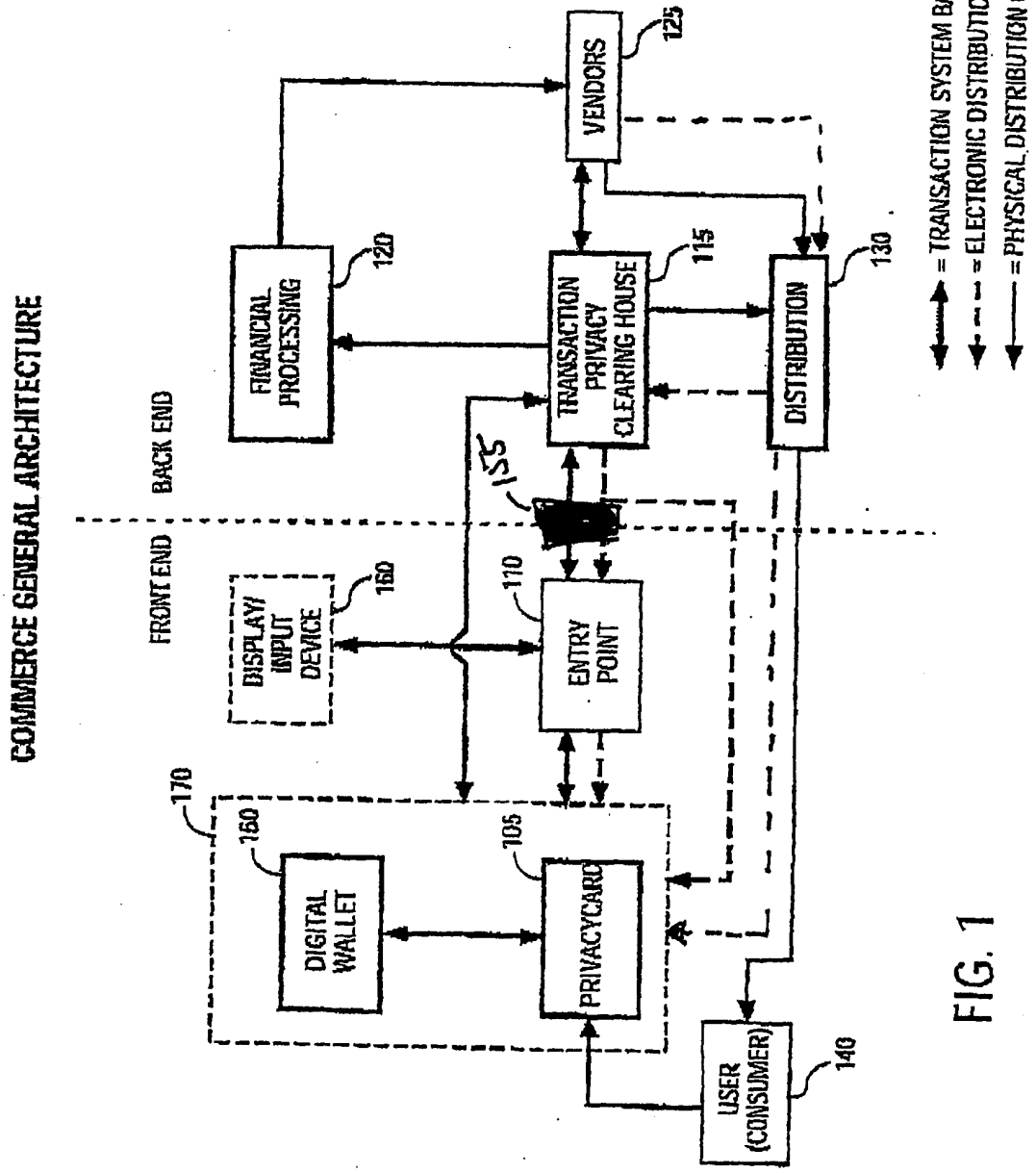

COMMERCE GENERAL ARCHITECTURE
BACK END
FRONT END
FINANCIAL PROCESSING
120
VENDORS
125
TRANSACTION PRIVACY CLEARING HOUSE
115
DISTRIBUTION
130
155
DISPLAY/ INPUT DEVICE
160
110
ENTRY POINT
170
160
DIGITAL WALLET
105
PRIVACYCARD
USER (CONSUMER)
140
= TRANSACTION SYSTEM BACKBONE
= ELECTRONIC DISTRIBUTION CHANNEL
= PHYSICAL DISTRIBUTION CHANNEL

FIG. 1

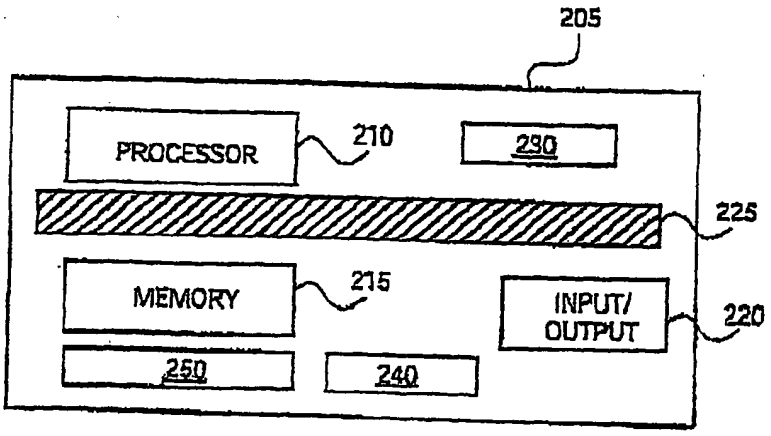

205
PROCESSOR
210
290
225
MEMORY
215
INPUT/
OUTPUT
220
250
240

FIG. 2

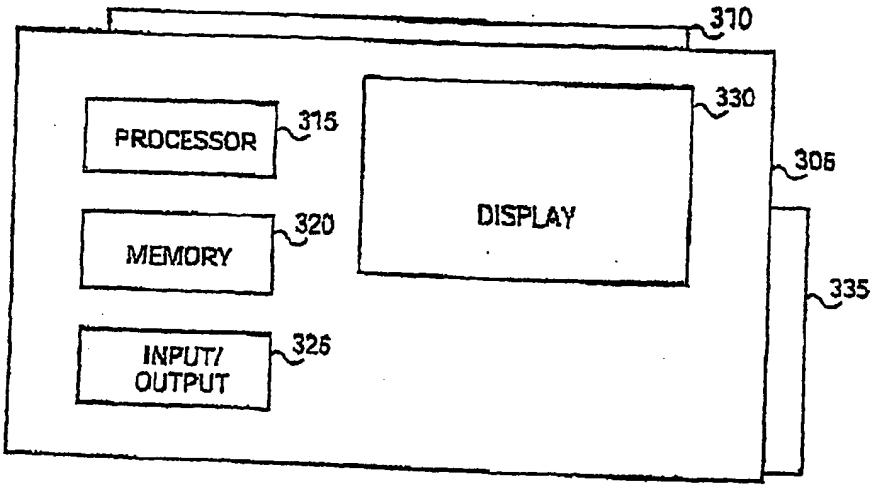

370
PROCESSOR
315
330
DISPLAY
306
MEMORY
320
335
INPUT/
OUTPUT
325

FIG. 3

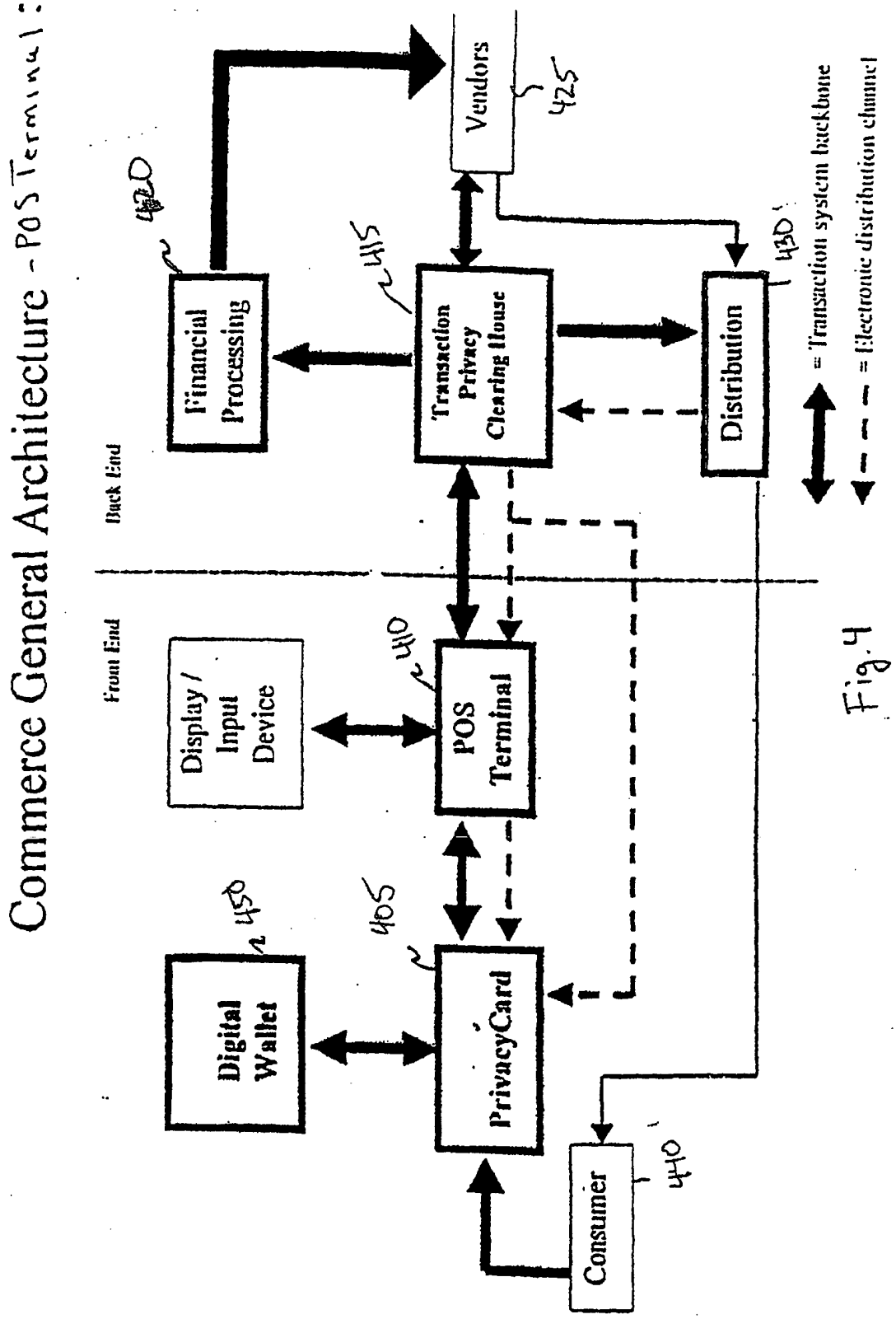
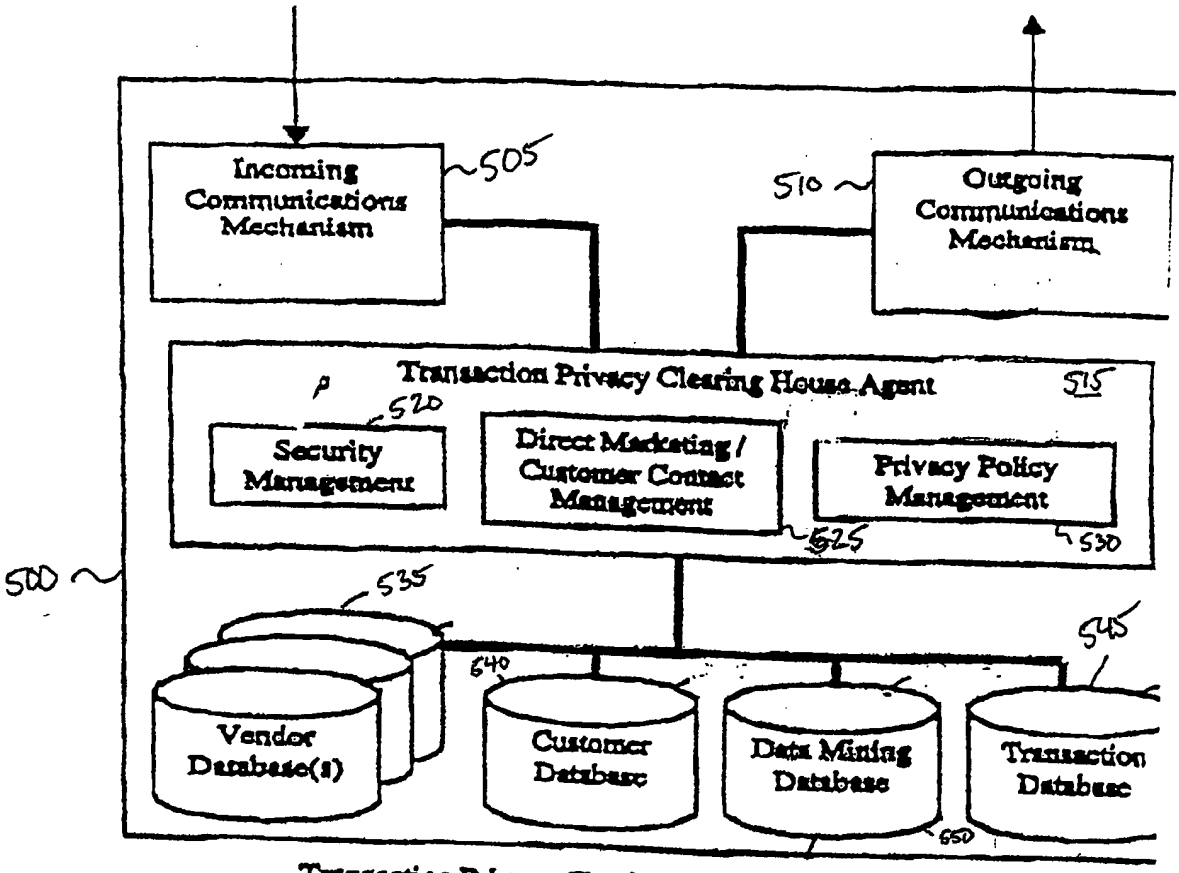

Commerce General Architecture - POS Terminal:
Back End
Front End
Vendors
425
420
Financial Processing
415
Transaction Privacy Clearing House
430
Distribution
= Transaction system backbone
= Electronic distribution channel
Display / Input Device
410
POS Terminal
450
Digital Wallet
405
PrivacyCard
440
Consumer

Fig. 4



Transaction Privacy Clearing House: Major Components

Figure 5

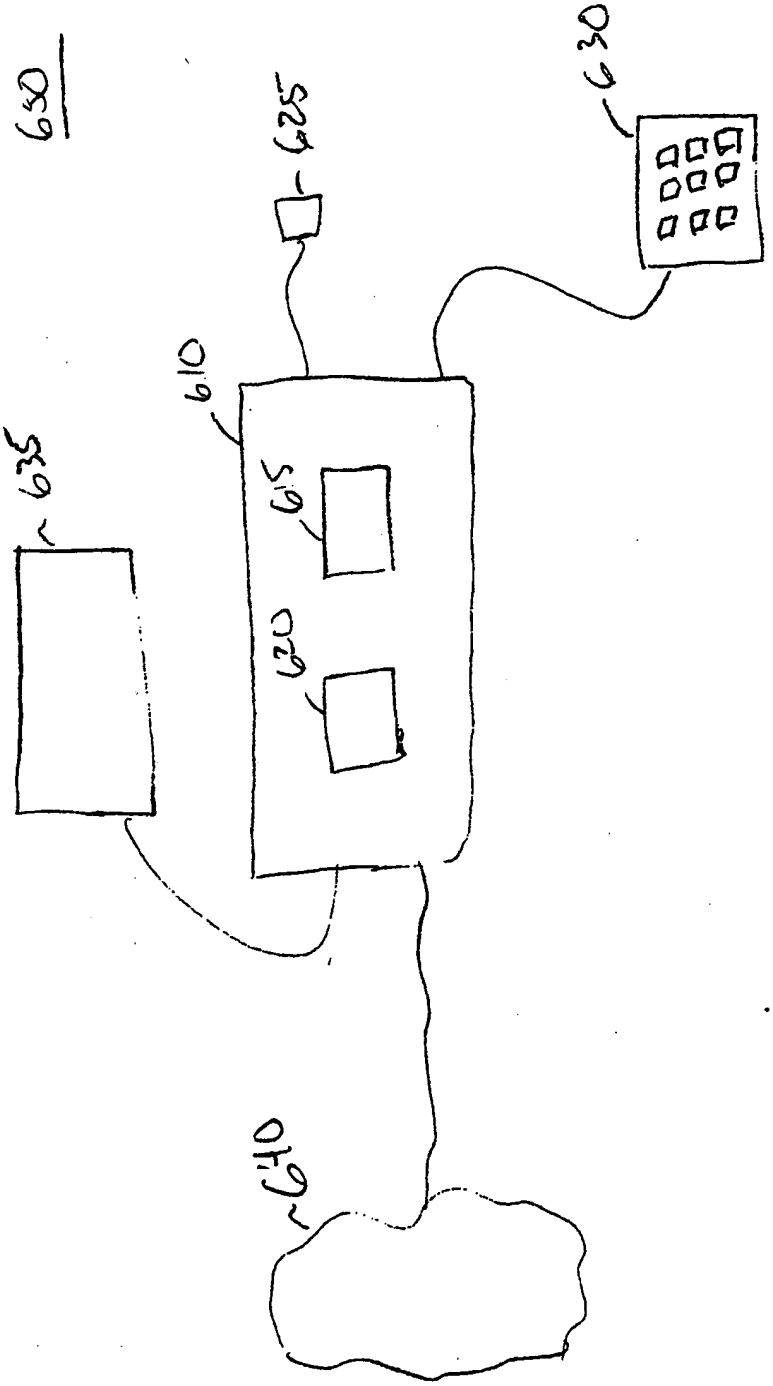


Figure 6

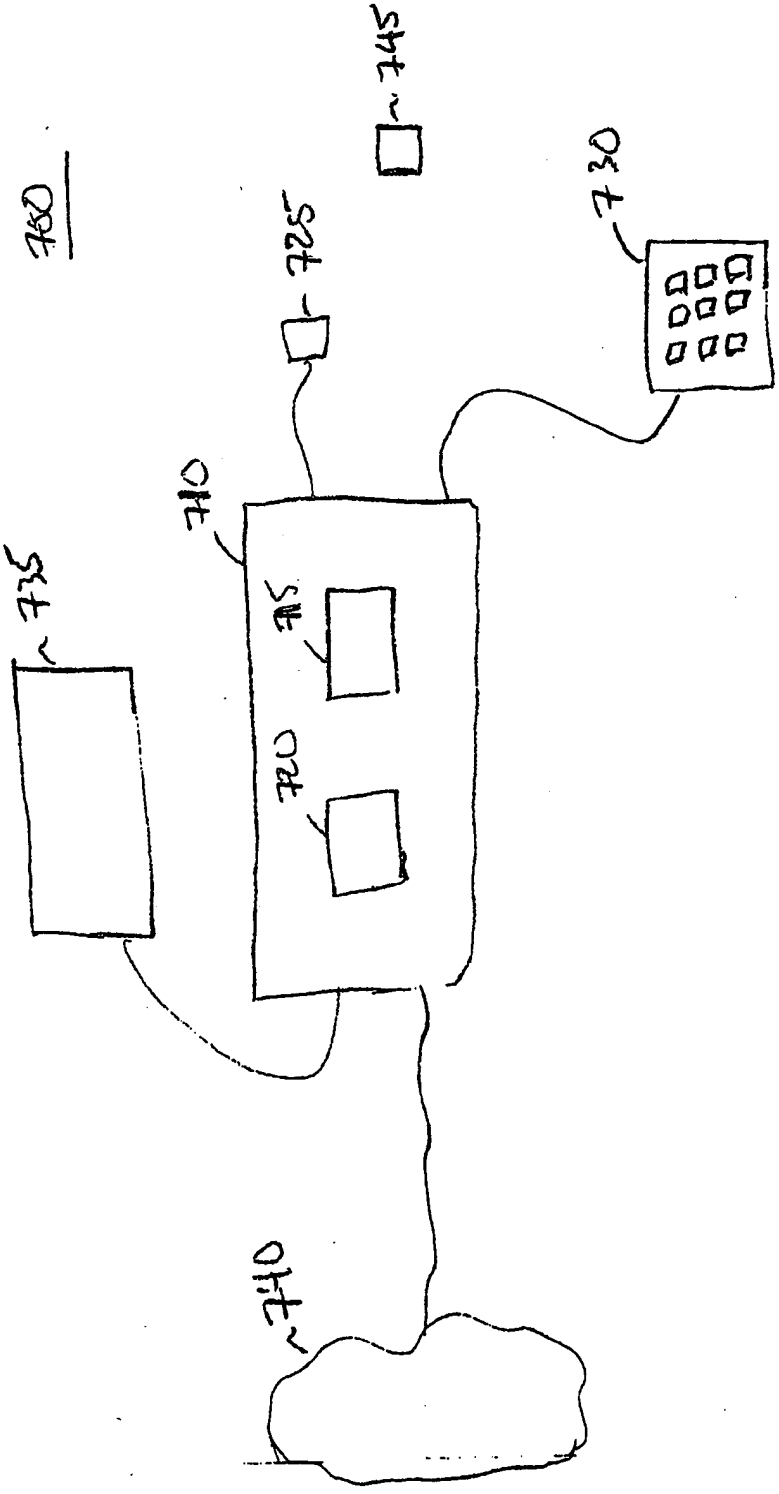


Figure 7

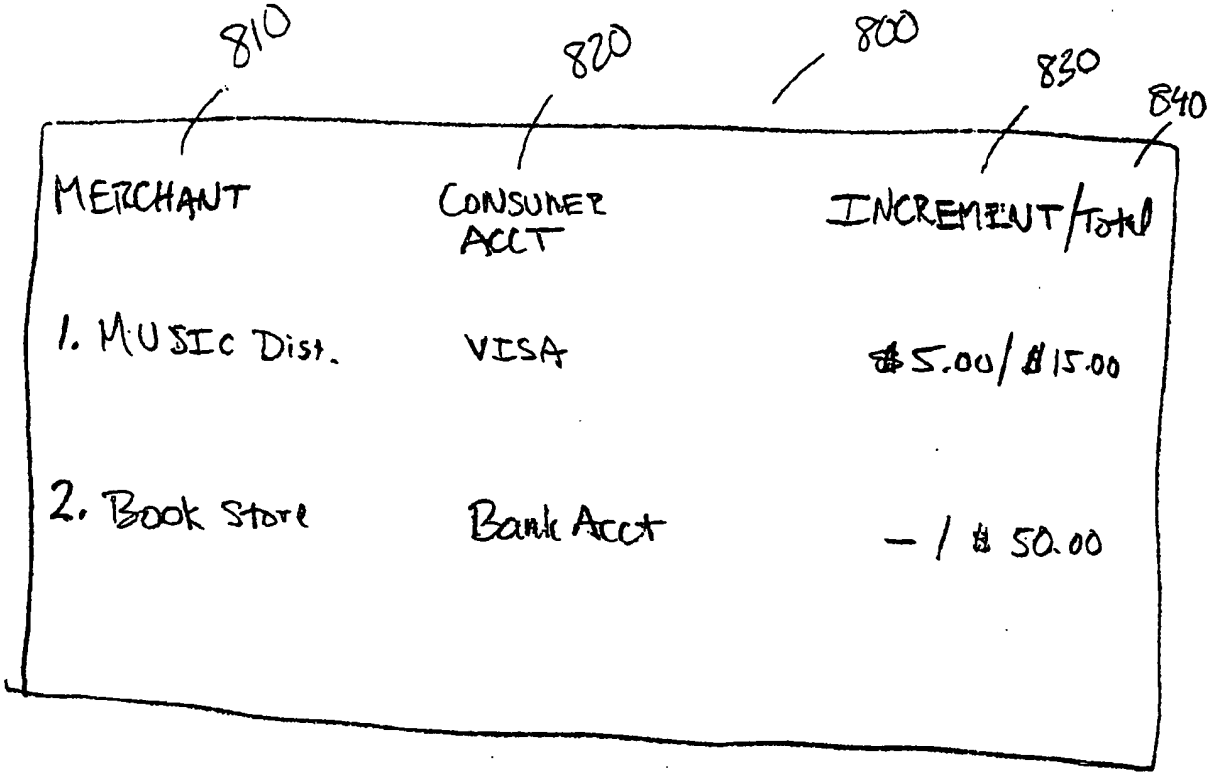

810
820
800
830
840
MERCHANT
CONSUMER ACCT
INCREMENT/Total
1. MUSIC Dist.
VISA
$5.00/$15.00
2. Book Store
Bank Acct
—/$50.00

Figure 8

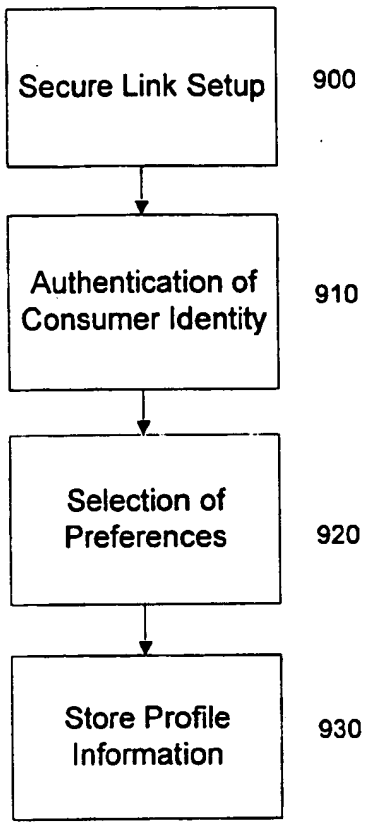

Secure Link Setup
900
Authentication of Consumer Identity
910
Selection of Preferences
920
Store Profile Information
930

Figure 9

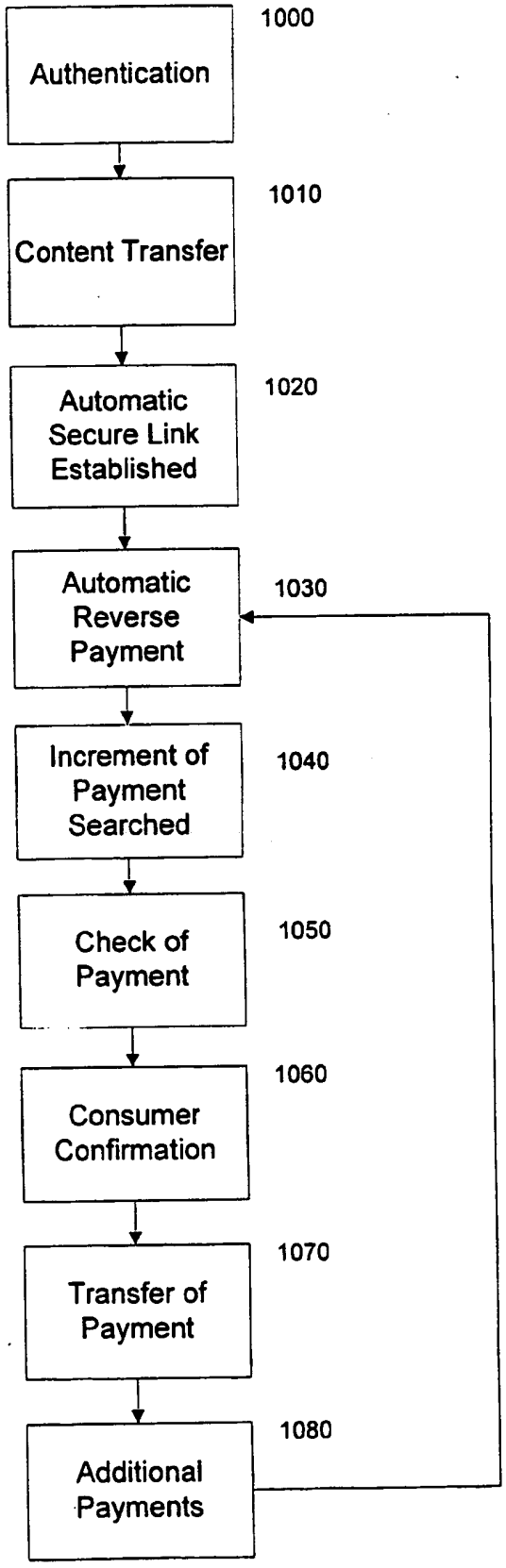

Authentication
1000
Content Transfer
1010
Automatic Secure Link Established
1020
Automatic Reverse Payment
1030
Increment of Payment Searched
1040
Check of Payment
1050
Consumer Confirmation
1060
Transfer of Payment
1070
Additional Payments
1080

Figure 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/16801

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/32
US CL : 713/202
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/202; 380/23,29; 463/29,411

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,970,143 A (SCHNEIER et al.) 19 October 1999 (19.10.1999), abstract, column 10, lines 10-49, column 22, lines 17-14, Fig. 1A , Fig.2, Fig 3, (reference elements 31,34), column 11, lines 56-67, column 23, lines 26-40, Fig. 8A (reference elements 111-122, 110-130),column 25, lines 40-67, column 26, lines 54-67 through column 27, lines 1-52, column 77, lines 54-67 through column 78, lines 1-10.	1-19
Y,P	US 2002/0025851 A1 (FRANKULIN et al.) 28 February 2002 (28.02.2002),Fig. 1, Fig. 3, pg.1 , paragraphs 6-7, pg.2, paragraphs 14-23.	1,7,12
Y	US 5,083,271 A (THACHER et al.) 21 January 1992 (21.01.1992), the entire document.	1,7,12
Y	US 5,229,764 A (MATCHETT et al.) 20 July 1993 (20.07.1993), the entire document.	1,7,12

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 July 2002 (12.07.2002)	08 AUG 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Gail O Hayes for James R. Matthews Telephone No. (703) 305-4274

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US02/16801

Continuation of B. FIELDS SEARCHED Item 3:
WEST, DIALOG, ProQuest, Dogpile. Search terms: secure console, gaming and biometric, authentication or PIN or password